

**Notice of Allowability**

Application No.

09/930,349

Examiner

Minh Dinh

Applicant(s)

MARUYAMA ET AL.

Art Unit

2132

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 1/25/05 and examiner's amendment on 4/21/05.
2. ☒ The allowed claim(s) is/are 1-24 and 26-37.
3. ☒ The drawings filed on 15 August 2001 are accepted by the Examiner.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All    b) ☐ Some\*    c) ☐ None    of the:
  1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☒ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |   |
|---|---|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)                       |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                | 6. <input checked="" type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                               |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material          | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance              |
|   | 9. <input type="checkbox"/> Other _____.  |

### **EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Wayne Ellenbogen on 4/21/2005.

The application has been amended as follows:

1. (Currently Amended) A digital signature method comprising the steps of:  
generating, by an third party agent mediating an electronic transaction between a signature demandant and a signatory, summary text from an electronic document to be signed which is received from the signature demandant, the summary text including essential information to be confirmed relating to the electronic transaction;  
displaying said summary text on a display screen of a terminal of the signatory;  
calculating, in the terminal, a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;  
encrypting, in the terminal, data, including said digest value, using a private key stored in said terminal, and generating a signature value; and  
generating, by the agent, a signed document including said signature value.

2. (Original) The digital signature method according to claim 1, wherein said electronic document and said signed document are XML documents, and said summary text is generated using XPath of said electronic document, which is an XML document.

3. (Original) The digital signature method according to claim 1, wherein said terminal includes a signature template having a variable field, further comprising the steps of:  
adding said digest value to said variable field of said signature template;  
employing said function to convert said signature template to which said digest value has been added; and  
employing said private key to encrypt a value obtained by conversion and generating said signature value.

4. (Original) The digital signature method according to claim 3, wherein a URI for said electronic document is added to said variable field of said signature template.

5. (Original) The digital signature method according to claim 3, wherein said signature template is canonicalized using a predetermined algorithm.

6. (Original) The digital signature method according to claim 1, wherein said function is a hash function.

7. (Currently Amended) A digital signature system comprising:

~~an~~ a third party agent operative to mediate an electronic transaction between a signature demandant and a signatory, the agent being adapted to generate summary text from an electronic document to be signed, the document relating to the electronic transaction, the summary text including essential information to be confirmed relating to the electronic transaction;

a terminal ~~configurable for use by~~ of the signatory, the terminal including a display screen and means for displaying said summary text on the display screen, the terminal being operative: (i) to calculate a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult; and (ii) to encrypt data, including said digest value, using a private key stored in said terminal; and

means for generating, by the agent, a signed document including a signature value corresponding to the encrypted data generated by the terminal.

8. (Original) The digital signature system according to claim 7, wherein said electronic document and said signed document are XML documents, further comprising:

means for generating said summary text using XPath of said electronic document, which is an XML document.

9. (Original) The digital signature system according to claim 7, wherein said terminal includes a signature template having a variable field, further comprising:

means for adding said digest value to said variable field of said signature template;  
means for employing said function to convert said signature template to which said digest value has been added; and  
means for employing said private key to encrypt a value obtained by conversion.

10. (Original) The digital signature system according to claim 9, wherein a URI for said electronic document is added to said variable field of said signature template.

11. (Original) The digital signature system according to claim 9, wherein said signature template is canonicalized using a predetermined algorithm.

12. (Original) The digital signature system according to claim 7, wherein said function is a hash function.

13. (Currently Amended) A digital signature method comprising the steps of:  
a signature demandant transmitting an electronic document to an a third party agent mediating an electronic transaction between the signature demandant and a signatory;  
said agent generating summary text from said electronic document, and transmitting said summary text to a terminal of the signatory, the summary text including essential information to be confirmed relating to the electronic transaction;  
said signatory displaying said summary text on a display screen of said terminal of said signatory;  
said signatory confirming said summary text, and employing a private key stored in said terminal to digitally sign at least one of said summary text and a document corresponding to said summary text;  
said signatory transmitting, to said agent, a signature value generated by the digital signature;  
said agent generating a signed document by adding said signature value to said electronic document; and  
said agent transmitting said signed document to said signature demandant.

Art Unit: 2132

14. (Currently Amended) A digital signature system comprising:

means for permitting a signature demandant to transmit an electronic document to an a third party agent mediating an electronic transaction between the signature demandant and a signatory;

means for permitting said agent to generate summary text from said electronic document, and to transmit said summary text to a terminal of the signatory, the summary text including essential information to be confirmed relating to the electronic transaction;

means for permitting said signatory to display said summary text on a display screen of said terminal of said signatory;

means for permitting said signatory to confirm said summary text, and to employ a private key stored in said terminal to digitally sign at least one of said summary text and a document corresponding to said summary text;

means for permitting said signatory to transmit, to said agent, a signature value generated by the digital signature;

means for permitting said agent to generate a signed document by adding said signature value to said electronic document; and

means for permitting said agent to transmit said signed document to said signature demandant.

15. (Currently Amended) A digital signature mediation method comprising the steps of:  
receiving an electronic document from a signature demandant;

an a third party agent receiving the electronic document and generating summary text from said electronic document, the agent mediating an electronic transaction between the signature demandant and the signatory, the summary text including essential information to be confirmed relating to the electronic transaction;

the agent transmitting said summary text to a terminal of a signatory;

the agent generating a signed document by adding, to said electronic document, a signature value received from said terminal of said signatory, and

transmitting said signed document to said signature demandant.

16. (Original) The digital signature mediation method according to claim 15, wherein said electronic document and said signed document are XML documents, and said summary text is generated using XPath of said electronic document, which is an XML document.

17. (Currently Amended) A digital signature mediation system comprising:  
means for receiving an electronic document from a signature demandant;  
means for generating, by an a third party agent mediating an electronic transaction between the signature demandant and a signatory, summary text from said electronic document;  
means for transmitting, by the agent, said summary text to a terminal of the signatory;  
means for generating, by the agent, a signed document by adding, to said electronic document, a signature value received from said terminal of said signatory; and  
means for transmitting said signed document from the agent to said signature demandant.

18. (Original) The digital signature mediation system according to claim 17, wherein said electronic document and said signed document are XML documents, further comprising:  
means for generating said summary text using XPath of said electronic document, which is an XML document.

19. (Currently Amended) An information terminal for use by of a signatory, the information terminal comprising:  
means for receiving summary text generated by an a third party agent mediating an electronic transaction between a signature demandant and the signatory from an electronic document to be signed relating to the electronic transaction;  
means for displaying said summary text on a display screen of the terminal;  
means for calculating a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;  
storage means for storing a private key;  
means for employing said private key to encrypt data, including said digest value; and

means for generating a signature value obtained by the cryptography

20. (Original) The information terminal according to claim 19, further comprising:
- storage means for storing a signature template having a variable field;
  - means for adding, to said variable field of said signature template, said digest value, a URI of said electronic document and other information concerning said electronic document;
  - means for employing said function to convert said signature template to which said digest value and said information have been added; and
  - means for employing said private key to encrypt a value obtained by conversion, and generating said signature value.

21. (Original) The information terminal according to claim 20, wherein said electronic document is an XML document, and said signature template is canonicalized using a predetermined algorithm.

22. (Currently Amended) A digital signature method comprising the steps of:
- receiving summary text generated by an a third party agent mediating an electronic transaction between a signature demandant and a signatory from an electronic document to be signed relating to the electronic transaction;
  - displaying said summary text on a display screen of a terminal of the signatory;
  - calculating, in the terminal, a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;
  - encrypting, in the terminal, data, including said digest value by employing said private key that is recorded in a storage area of an information terminal, or in a storage area of a memory connectable to said information terminal; and
  - generating a signature value obtained by the cryptography.

23. (Original) The digital signature method according to claim 22, further comprising:



Art Unit: 2132

adding said digest value, a URI of said electronic document and other information concerning said electronic document to a variable field of a signature template, which that is recorded in said storage area of said information terminal or in a storage area of a memory connectable to said information terminal;

employing said function to convert said signature template to which said digest value and said information have been added; and

employing said private key to encrypt a value obtained by conversion, and generating said signature value.

24. (Original) The digital signature method according to claim 23, wherein said electronic document is an XML document, and said signature template is canonicalized using a predetermined algorithm.

25. (Canceled)

26. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

27. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

28. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing digital signature mediation, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 15.

29. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 1.

30. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 13.

31. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 15.

32. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 7.

33. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 14.

34. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature mediation system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 17.

35. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing an information terminal, the

computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 19.

36. (Original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

37. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 22.

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method and system for a first party (a signature demandant) sending an electronic document to a second party (a signatory) requesting a digital signature of the electronic document from the second party. More specifically, the independent claims identify the uniquely distinct features of utilizing a third party agent who receives the electronic document to be signed from the signature demandant, generates summary text from the electronic document for the signatory to sign using his/her terminal, and generates a signed document including the signatory's signature value of the summary text. The closest prior art, Brown et al. (6,671,805), discloses an agent who uses relevant information in one document to generate another document to be signed. However, Brown does not teach that the agent generates summary text from a document. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a

rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

3. The new declaration filed 1/25/2005 is deficient. It lists the application number 2003-262955 as foreign priority. However, the number listed in the declaration originally filed and in the certified copy of the foreign application is 2000-262955. Correction is required.

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,671,279 to Elgamal

U.S. Patent No. 5,903,878 to Talati et al.

U.S. Patent No. 6,003,015 to Kang et al.

U.S. Patent No. 6,039,248 to Park et al.

U.S. Patent No. 6,085,322 to Romney et al.

Art Unit: 2132

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802.

The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
4/25/05

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100